VMware vDefend Advanced Threat Prevention

Rapidly Respond to Ransomware and Advanced Threats

Key benefits

Efficient operation: ATP combines multiple related alerts across many different assets and hops into a single intrusion campaign view. This view enables the incident response team to quickly understand the scope of the threat and prioritize its response. Further, the information ATP provides allows security teams to proactively hunt for network threats. Finally, the solution reduces false positives.

High-fidelity detection: ATP detects not only known threats but also new, evolving threats that have never been seen before. It is engineered to detect malware specifically designed to evade standard security tools. ATP detects threats by analyzing local network traffic behavior, and importing and utilizing indicators of malicious behavior from the VMware global threat intelligence network.

Deep threat visibility: ATP has complete visibility into north-south and east-west traffic. Thus, ATP provides a comprehensive overview of abnormal behavior across the network. It also extends protection to all assets in the infrastructure, including those devices that do not have endpoint protection installed, such as physical servers with legacy workloads.

Continued on page 2.

At a glance

VMware's vDefend Advanced Threat Prevention (ATP) provides network security capabilities that protect organizations against advanced threats, including ransomware.

VMware vDefend ATP combines multiple detection technologies – Intrusion Detection/ Prevention System (IDS/IPS), Malware Prevention Service, and Network Traffic Analysis (NTA) with aggregation, correlation, and context engines from Network Detection and Response (NDR). Also included is an NDR Sensor that analyzes threat activities across non-vSphere environments, providing comprehensive datacenter-wide threat detection. ATP with Intelligent Assist for vDefend, powered by GenAI and LLM, democratizes threat response by simplifying how virtualization, network security, and SOC teams understand detailed, contextual information about active threats and their impact.

These capabilities complement each other to provide a cohesive defensive layer, with every event mapped to the MITRE ATT&CK framework for clearer threat context in a powerful visual interface. As a result, ATP increases detection fidelity, reduces false positives, and accelerates remediation while reducing the manual work for security analysts.

Advanced Threat Prevention

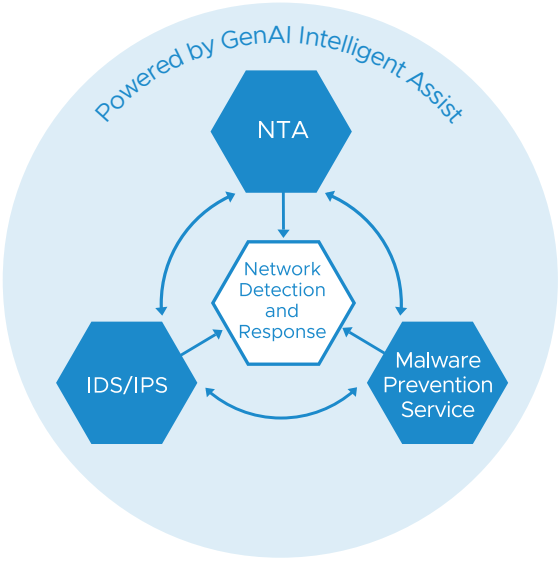

Figure 1: VMware Advanced Threat Prevention = IDS/IPS + Malware Prevention Service + NTA + Network Detection and Response powered by GenAI with Intelligent Assist

vmware by Broadcom

Key benefits (continued)

Rapid triage and threat remediation: Coalesce multiple related alerts across many different assets and hops into a single intrusion campaign, enabling your SOC teams to quickly scope the threat and prioritize its remediation. Intelligent Assist for VMware vDefend, powered by GenAI, offers a conversational chatbot interface to investigate and remediate threats efficiently. It enables virtualization, network security and SOC teams to get detailed contextual information about active threat campaigns thus reducing time-to-detection significantly.

Key capabilities

IDS/IPS

This technology inspects all traffic that enters or leaves the network, detecting and preventing known threats from gaining access to the network, critical systems, and data. Built directly into the hypervisor, the IDPS requires no discrete appliances, making it simpler to deploy, network-agnostic, and ensuring policies follow workloads. Protection can be applied at the granularity of each workload's vNIC. With Turbo mode architecture, IPS throughput performance scales to address the evolving bandwidth needs of the private cloud. Federation support allows large enterprises to incorporate a Global manager as well as multiple Local Managers to manage geographically dispersed locations. Additionally, custom IPS signatures enable customers to extend protection by adding signatures specific to the threats faced in their environment.

Network Traffic Analysis (NTA)

Network Traffic Analysis (NTA) offers behavior-based threat detection, effectively complementing traditional signature-based methods. By continuously monitoring network flows and employing machine learning algorithms alongside advanced statistical tech-niques, NTA establishes a baseline for normal behavior across diverse protocols, hosts, and applications. This proactive approach allows NTA to identify subtle indicators of compromise—such as DNS tunneling, port scanning, beaconing, and data exfiltration—that signature-based systems might overlook. The result is a reduction in false positives, improved visibility, and enhanced capabilities for security teams to detect and contain advanced attacks earlier in the kill chain.

VM-aware Malware Prevention Service (MPS)

MPS is an advanced engine designed for malware analysis and prevention across both file based and fileless malware, utilizing a multi-technique approach. It integrates machine learning, static and dynamic analysis, and memory analysis to safeguard organizations against highly evasive zero-day malware. MPS features a unique Guest Introspection capability that operates on each hypervisor to deliver deep visibility into file systems and processes across all hosts. It enables analysis of encrypted files, supports fileless script-based buffer analysis to detect in-memory attacks and reduce risk from evasive threats, enhances threat detection and response, and strengthens overall security posture. MPS also supports a wide range of operating systems, including Windows, RHEL, SLES, CentOS, and Red Hat Linux, and is capable of analyzing over 100 different file types, ensuring broad protection across diverse enterprise environments.

Multi-context Network Detection and Response (NDR)

Network Detection and Response (NDR) combines a powerful aggregation, correlation, and context engine to deliver comprehensive threat visibility. It collects and normalizes signals from multiple detection technologies - IDS/IPS, MPS, NTA - to determine whether network activity is malicious or benign. NDR also links related alerts into a unified intrusion

Use cases

Virtual patching: Proactively protect vulnerable workloads using distributed IDS/IPS, allowing security teams time to plan and deploy patches to workloads.[1]

Compliance: Simplify audits and quickly bring environments into compliance (PCI, HIPAA, etc.) by deploying a software-based, distributed IDS/IPS with minimal changes to your existing network.

Threat Investigation: Empower SOC teams to visualize attack chains by leveraging multi-context NDR, which consolidates alerts into curated threat campaigns. These campaigns are enriched with contextual information and mapped to MITRE ATT&CK techniques and TTPs, providing clear explainability and deeper insights into the attacker's behavior.

Ransomware Prevention and Recovery: Advanced Threat Prevention identifies, prevents, and detects ransomware activity. After a ransomware event, VMware Live Recovery can help to recover data from the last known clean backup safely.[2]

1,2. Requires VMware vDefend Advanced Threat Prevention.

campaign, providing security analysts with rich context and actionable Indicators of Compromise (IOC's) for faster threat investigation and response.NDR integrates seamlessly with SIEM platforms to provide clear visibility into ransomware and lateral movement across east–west traffic, sending correlated alerts and campaign insights instead of raw data to simplify downstream analysis and accelerate threat response.

NDR Sensor

The NDR Sensor delivers advanced, out-of-band threat detection for non-virtualized environments. Deployed as a lightweight virtual appliance, it monitors mirrored network traffic in real time, without impacting application performance. Using behavioral analytics, signature detection, and file inspection, it provides deep visibility into anomalies, malware, and advanced threats. Designed for fast deployment and flexibility, the NDR Sensor extends protection to non-vSphere workloads and integrates with ATP for a single, unified view across your private cloud.

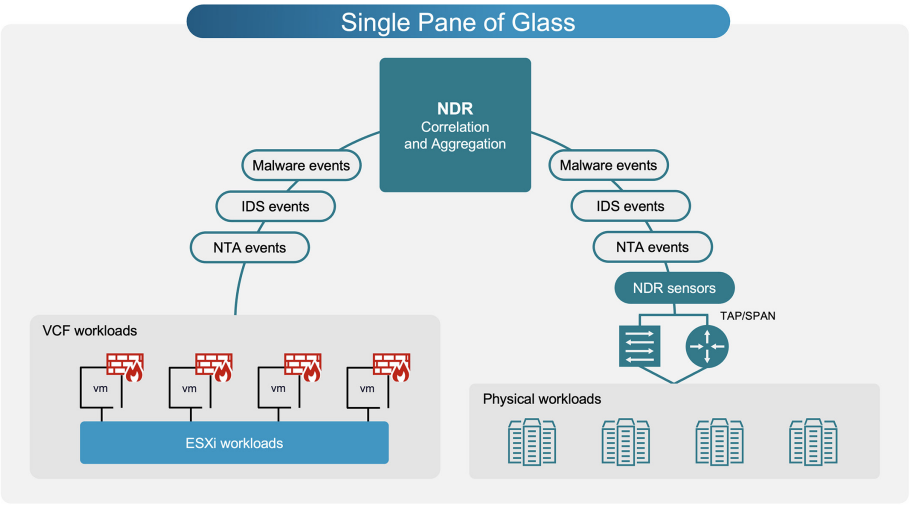

Figure 2: NDR Sensor and VMware vDefend Firewall with Advanced Threat Prevention

Advanced Threat Prevention Capabilities

	vDefend Distributed Firewall with ATP	vDefend Gateway Firewall with ATP	vDefend NDR Sensor
Core Use Case	Micro-segmentation with Advanced Threat Detection and Prevention	Zone-segmentation with Advanced Threat Detection and Prevention	Threat Detection
Deployment Form Factor	In-Hypervisor	VM or ISO	VM (Switch SPAN/RSPAN or Gigamon/NetScout)
Traffic Mode	Inline	Inline	Out of Band (listening only)
Intrusion Detection	✓	✓	✓
Intrusion Prevention	✓	✓	✗
Malware Detection	✓	✓	✓
Malware Prevention	✓	✗	✗
Network Traffic Analysis	✓	✗	✓
Network Detection & Response	✓	✓	✓

System requirements for NDR Sensor

Minimum resource requirements per NDR Sensor

Resource	Minimum Requirement
CPU	12 vCPU
Memory	24 GB
Storage	250 GB
Networking	2 interfaces

vmware® by Broadcom

Item No: VMware vDefend Advanced Threat Prevention_JR17 10/25